Auditiel

ScTools, Perso

Outil d'enrôlement de certificats EJBCA

Manuel d'installation et de configuration

Version 1.0.1

1 SOMMAIRE

1Sommaire..... 2
2Introduction..... 3
2.1Pré requis..... 3
2.2Versions..... 3
2.3Glossaire..... 3
3Installation..... 4
4Présentation..... 5
4.1Activation..... 5
4.2 Personnalisation..... 5
4.3Paramétrages..... 7

2 INTRODUCTION

2.1 Pré requis

Ce document s'adresse aux personnes désirant installer le programme de personnalisation de cartes. Ce programme, indépendant, permet de rechercher l'utilisateur dans un annuaire LDAP, puis d'enrôler un certificat EJBCA sur une carte à puce.

Dans la suite du document, il est fait référence aux cartes à puce. Cette dénomination comprend également les clés USB cryptographiques.

2.2 Versions

Version	Date	Auteur	Modification
1.0.0	26/04/2007	Jérôme DUSAUTOIS	Création
1.0.1	30/04/2007	Jérôme DUSAUTOIS	Modification pour utilisateur propriétés extension ScTools.

2.3 Glossaire

CA : Autorité de certification.

EJBCA : PKI Open Source en JAVA, basée sur le serveur d'applications JBOSS.

Carte à puce : Carte plastique respectant la norme 7816 et équipé d'un mirco-processeur cryptographique.

Clé USB : Clé USB disposant d'un micro-processeur cryptographique.

3 INSTALLATION

L'installation s'effectue en utilisant le package d'installation de ScTool. La version ScToolsEjb.msi est nécessaire, puisque cet outil est destiné à l'enrôlement de certificats EJBCA.

L'installation nécessite le framework 2.0 de Microsoft.

Le programme de perso se nomme PERSO.EXE. Il est copié, à l'installation, dans le répertoire système (\Windows\Sytem32).

Pour lancer le programme, cliquez sur le bouton démarrer, puis le choix Exécuter. Entrez la commande Perso puis validez.

4 PRÉSENTATION

4.1 Activation

Au lancement du programme, l'écran suivant apparaît.

Personnalisation des cartes (eDirectory-EJBCA)
Entrez le début du nom à rechercher dans la base, puis cliquez sur le bouton Rechercher. Le caractère * permet de lister l'ensemble des noms. Le nombre de noms listés est limité à 100.
Nom à rechercher dans eDirectory
Rechercher
Sélectionnez l'utilisateur pour lequel vous désirez enregistrer un certificat dans la carte, puis cliquez sur le bouton Personnaliser.
Paramètres
Personnaliser
Quitter

La zone de recherche permet de saisir le début du nom commun de l'utilisateur. Dès le premier caractère, le bouton Rechercher s'active. La base de recherche dans eDirectory est fixée dans les paramètres.

Lorsque le bouton Rechercher est sélectionné, la liste des utilisateurs correspondant s'affiche. Seuls les 100 premiers utilisateurs sont affichés.

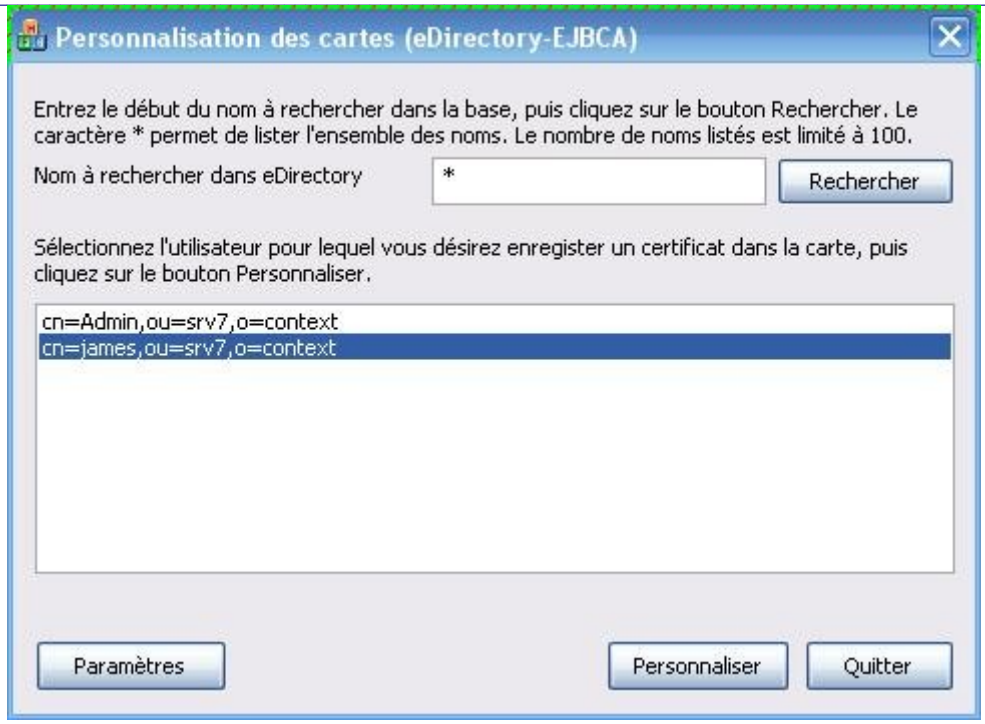
La sélection d'un utilisateur dans la liste active le bouton Personnaliser.

4.2 Personnalisation

La personnalisation d'une carte consiste en l'inscription d'un certificat. Le certificat est demandé à EJBCA. Les informations du certificat sont obtenues de l'annuaire eDirectory. Les informations suivantes sont incluses dans la demande de certificat :

- Le DN de l'utilisateur
- Le mail de l'utilisateur.

Après la recherche, l'écran principal ressemble à l'image suivante.


Personnalisation des cartes (eDirectory-EJBCA)
Entrez le début du nom à rechercher dans la base, puis cliquez sur le bouton Rechercher. Le caractère * permet de lister l'ensemble des noms. Le nombre de noms listés est limité à 100.
Nom à rechercher dans eDirectory
*
Rechercher
Sélectionnez l'utilisateur pour lequel vous désirez enregistrer un certificat dans la carte, puis cliquez sur le bouton Personnaliser.
cn=Admin,ou=srv7,o=context
cn=james,ou=srv7,o=context
Paramètres
Personnaliser
Quitter

Si le registre PropSheet dans la clé HKLM\Software\Auditiel\ScPerso contient la valeur 0, la personnalisation est immédiate. S'il contient la valeur 1, la page de propriété de l'extension de la mmc « Utilisateurs et ordinateurs Active Directory » s'affiche.

4.2.1 Registre PropSheet à 0

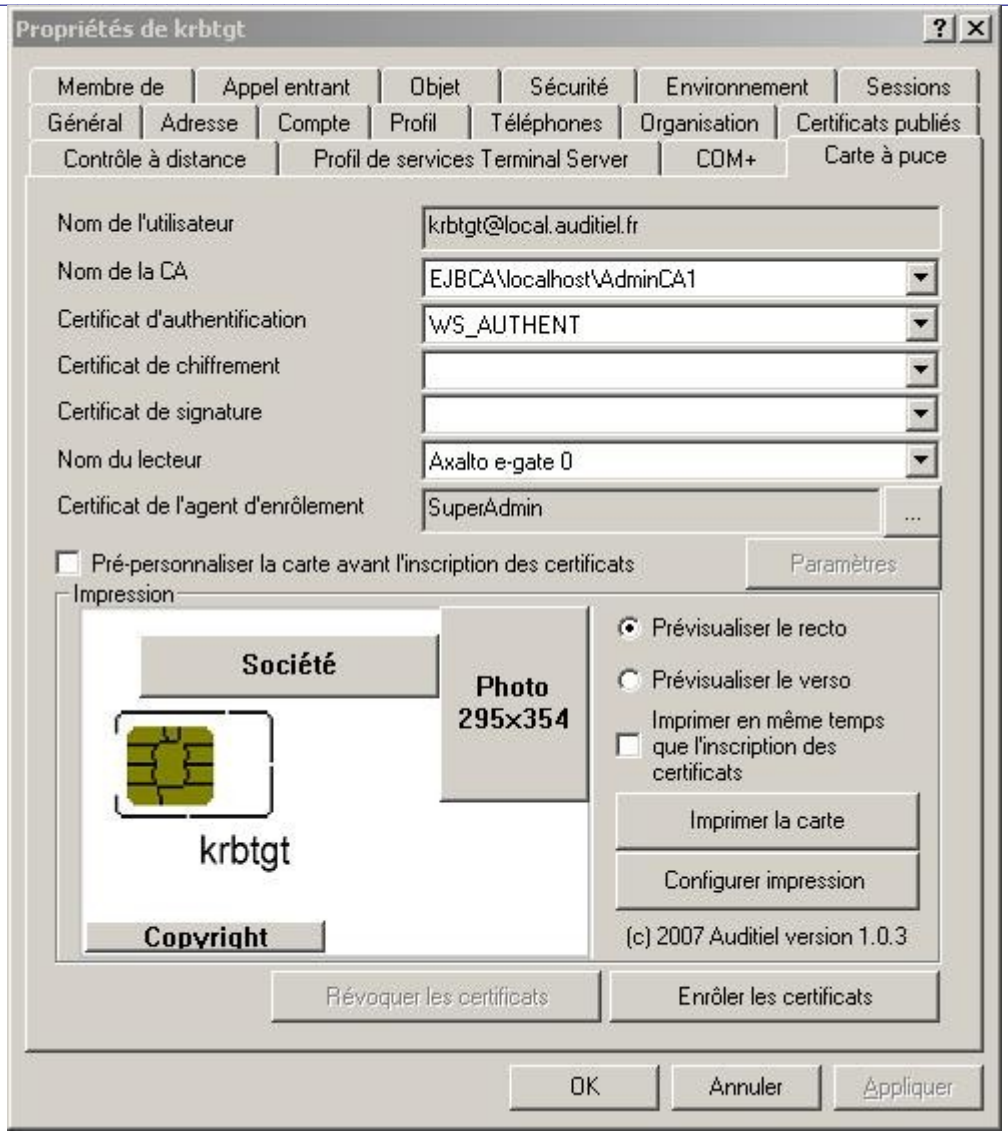
Lorsque le bouton Personnaliser est sélectionné, le pointeur de la souris affiche un sablier le temps de l'inscription du certificat. Cette action peut durée plusieurs secondes.

A l'issue de l'inscription, l'utilisateur est ôté de la liste et le bouton Personnaliser est désactivé.

Si une erreur se produit lors de la personnalisation, un message indique le type d'erreur rencontré. Dans ce cas, l'utilisateur n'est pas enlevé de la liste.

4.2.2 Registre PropSheet à 1

La fenêtre suivante d'affiche.



Le fonctionnement est le même que pour l'extension de la console mmc. Reportez vous à la documentation ScToolsInstallation.pdf pour de plus amples informations.

4.3 Paramétrages

Les paramètres du programme sont modifiés à partir de l'écran affiché lorsque le bouton Paramètres est sélectionné. Tous les paramètres sont sauvegardés dans la base de registre de l'utilisateur courant.

Les paramètres se découpent en trois groupes.

1. Paramètres eDirectory.
2. Paramètres EJBCA.
3. Paramètres carte.

L'écran suivant s'affiche lorsque le bouton Paramètres est sélectionné.

Le bouton Enregistrer permet de sauvegarder les paramètres dans le registre.

4.3.1 Paramètres eDirectory

Adresse du serveur : Entrez l'adresse IP:numéro de port, ou le nom DNS du serveur eDirectory à consulter pour la recherche des utilisateurs. Le port par défaut est le port 636. Si le numéro de port est spécifié et qu'il est de 389, la connexion n'est pas sécurisée. Dans les autres cas, la connexion est obligatoirement de type SSL. Le certificat du serveur n'est pas vérifié.

Base de recherche : Entrez la base de recherche dans eDirectory. Cette base permet de limiter le champ d'action de la fonction de recherche.

Nom de l'administrateur : Entrez le nom d'administrateur utilisé pour rechercher les informations dans eDirectory. L'accès à l'annuaire se fait uniquement en lecture.

Mot de passe : Entre le mot de passe correspondant à l'administrateur nommé ci-dessus.

4.3.2 Paramètres EJBCA

Ces paramètres ne sont pas accessibles si le registre PropSheet de la clé HKLM\Software\Auditiel\ScPerso est à 1.

Adresse du serveur : Entrez l'adresse du serveur hébergeant la PKI EJBCA. Entrez l'adresse IP ou le nom DNS du serveur. Cette adresse est automatiquement complétée par le numéro de port et le chemin suivant *:8443/ejbca/ejbcaws/ejbcaws*. La connexion est obligatoirement sécurisée SSL.

Nom de la CA : Entrez le nom de la CA à utiliser dans EJBCA.

Certificat d'administrateur : Sélectionnez, en utilisant le bouton à droite du champ, dans le magasin de l'utilisateur courant, le certificat d'administration EJBCA à utiliser. Le certificat doit être valide. La chaîne de certification est vérifiée.

Nom du modèle de certificat : Entrez le nom du modèle à utiliser pour générer le certificat sur EJBCA.

Autoriser le séquestre de la clé : Si cette case est cochée, la demande de certificat est une demande de génération de P12 de la part de EJBCA. Dans ce cas, EJBCA a l'opportunité de réaliser un séquestre de la clé privée. Si cette case n'est pas cochée, la clé privée est générée par la carte et ne peut donc pas être séquestrée par la PKI.

Remarque : Pour créer l'utilisateur sur EJBCA, le programme de personnalisation utilise le profil d'utilisateurs WS_USERS. Ce nom de profil n'est pas paramétrable. Le profil doit contenir les champs présents dans la demande de certificat. Le nombre et la nature de ces champs dépendent du schéma de l'annuaire. Dans notre exemple, les champs suivants doivent être présents.

- Cn (obligatoire sur EJBCA)
- Ou
- O

Le profil peut contenir plus de champs optionnels. Par contre, s'il manque un champ dans le profil WS_USERS, l'utilisateur ne pourra pas être créé.

4.3.3 Paramètres carte

Ces paramètres ne sont pas accessibles si le registre PropSheet de la clé HKLM\Software\Auditiel\ScPerso est à 1.

Nom du lecteur : Sélectionnez dans la liste des lecteurs installés sur la machine, le nom du lecteur à utiliser.